We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

4,800
Open access books available

122,000
International authors and editors

135M
Downloads

Our authors are among the

154
Countries delivered to

TOP 1%
most cited scientists

12.2%
Contributors from top 500 universities

CLARIVATE ANALYTICS BOOK CITATION INDEX INDEXED

WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com

34

Measuring Network Security

Emmanouil Serrelis and Nikolaos Alexandris
University of Piraeus
Greece

1. Introduction

The motive for this research has been the famous quote of Lord Kelvin "You can not improve what you can not measure". Today's information era has given new interpretations to this, expressing the need to measure abstract concepts such as Information Security. There are multiple sources, ranging from academic research to industrial reports, such as (Danahy, 2004), (Fisher, 2009) and (Sonnenreich et al., 2006) that share the same view and highlight the importance of measuring security within the context of Information Technologies.

This chapter provides the necessary information as well as the proper tools to measure the security of both IT Systems and business services are based on IT Systems. The main target of the methodologies that described is to provide a better way for managing the security of IT Systems and Infrastructures.

The first section of this chapter covers the basic requirements of any security measurement methodology. The second section of this chapter introduces a taxonomy of the existing security measurement methodologies. The third section highlights the limitations of the existing security measurement methodologies and supports that security should be calculated instead. The fourth and final section of the chapter elevates the need of new measurement methodologies for network security. New methodologies should be taking into account business needs apart from the traditional information technology requirements.

2. The need for security measurement

According to the American dictionary of Princeton the general definition of measurement is "*the act or process of assigning numbers to phenomena according to a rule*". Measurement has a very close relationship with metric which, according the same source, is a "*a system of related measures that facilitates the quantification of some particular characteristic*".

Focusing on the research area of IT (Maizlitsh, 2005) distinguishes between metrics that are used to quantify values that act as a control of proper functionality and those that act as a performance indicator. Security measurement is a topic that falls under the first category of controlling the proper functionality of security processes.

Although IT Security measurement is very interesting and useful topic in both academic and industrial environments, it deals with the quantification of an abstract concept. Similarly to any other abstract concept, security measurements tend to have rather vague implementations. This is justified by the fact that is hard to provide a figure that could express the current level of security. Thus, the difficulty of measuring security leads to the research of proper methodologies that could define the appropriate metrics as well as describe the necessary measurement process.
The expected benefits from the measurement of security are:

- Enable business strategy: IT Security is essential for the development and the support of trust between organizations, partners, customers and employees. This implies that there measuring the current level of security can held the alignment of business and technology strategies with security aspects and requirements.
- Support the daily business activities: Security measurement can accommodate the increases of the value of information and thus the increased risk levels related to each organizational asset.
- Facilitate risk management: The provision of a better toolset for managing risks can improve decision making as well as taking advantage of business opportunities.
- Reduce costs: A limited understanding of security status could lead to a high-cost operation of IT Systems and business processes, as well as to increased marketing and promotion expenses in order to "protect" the reputation of the products and the services of an organisation.
- Comply to regulatory and legal requirements: Being able to present and report the current status of security and risks is the basic condition for compliance.

A standardized approach of security measurement should aim to enable the operation of an organization without uncertainties or doubts, within a framework that could quantify the probability of a threat occurring, estimate the cost a potential damage, depict the performance overhead of the security processes and evaluate the effectiveness of security measures.

3. Requirements of security measurement methodologies

Having described the expected benefits of security measurement, this paragraph presents the necessary attributes of the security measurement methodologies, by interpreting business requirements in terms of IT Security. The adoption of those requirements if essential in order to make the measurement results utilizable.

A basic requirement is to enable envision to management in the section of security. Each measurement methodology should primarily intend to provide information that would depict the current status as well as the future trends from the security point of view. Additionally, the analysis of the security measurement should:

- Aid an analyst to diagnose the issues that are related to security and evaluate the performance of the existing mechanisms and processes.
- Quantify specific security characteristics and parameters.
- Easy the investigation of hypothetical and "before and after" scenarios.
- Focus the measurement interest to the causes, the media and the meaning of the results instead of the methodologies that were used.

According to (Jaquith, 2007) each measurement methodology should have as many of the following characteristics as possible:

- Consistently measured
- Cheap to gather
- Expressed as a number
- Uses at least one unit of measure
- Contextually specific
- Partial weight
- Repetitiveness
- Comparability

3.1 Consistently measured

The measurement methodologies provide reliability when they can be calculated with a reliable way. Different persons should be in position to apply the method and result the same answers using same set of data. The condition which is required to verify this, is expressed as follows: "Will two different individuals in which is submitted the same question give the same answer with regard to the measurement of some size?". These measurements should be differentiated from the "measurements" that they depend on the subjective crises of researchers and analysts that are reported as classifications, gradations or estimations.

A measurement methodology can ensure its consistence by recording the individual steps of measurement using a way that will be transparent and explicit to the person that will be asked to measure. Each measurement methodology should explain "how" each step should be applied and "why" it is applied with this particular way.

A particularly efficient way of maintaining consistence is the usage of questions of partial ignorance, that is to say questions that can be answered with "yes" or "no". Another way is the use of automated processes that would follow each time the same process of measurement without procedural divergences.

3.2 Cheap to gather

Each measurement methodology needs time in order to calculate the results. All measurement methodologies begin row data and afterwards, following the precise steps of each model, generate some useful information. Hence, initially, somebody or something should collect the data from a suitable source, convert them to the desirable form, and finally calculate and format the results.

An efficient measurement methodology should collect those steps of transformation and format using a unified and fast process. If the process of measurement is insufficient, the method of collection of data can cost time and money to the organisation, which could have been spent in the analysis of results.

The high cost of measurement methodology can be caused by a series of factors such as the frequency of measurements, the complexity of process and its non automated nature.

It is therefore reasonable for a model of measurement to also make proposals on the most optimal candidate sources of data, in the light of saving time and money

3.3 Expressed as a number

All measurements should be expressed as an absolute number or percentage, which represents something that measures a quantity of size. Gradations such as “high, intermediate, low” or “1, 2, 3” (from a third degree scale) represent relative grades but do not also measure any size, therefore they cannot be used in a proper model of measurement. Thus, “expressed as an absolute number” implies the number of total elements and not the number that expresses the order of total elements.

Thus, measurement methodologies that are not expressed as numbers are not suitable for the measurement of security. Indicators such as traffic lights with the three possible values “red, yellow, green” they do not constitute some type measurement since they do not include some kind of numerical scale.

It should be noted that the colors of traffic lights can be used as depiction or presentation of the current state but in a more abstract level accompanying the necessary numerical data that should remain the main objective of security measurement.

3.4 Uses at least one unit of measure

Another basic requirement of measurement models of security is that all the related measurements should also include a relative unit of measurement, which will characterize the sizes that are been measured. For instance, the measurement “number of natural invasions in the IT building” uses as a unit of measurement the invasions. With the use of units of measurement, the researcher knows how to express similar measurements using the same way.

In certain cases it is better to use more than one measurement units aiming to facilitate the comparison of different applications. In the previous example the more general measurement unit can be also mentioned as the “number of individuals that tried to invade in the IT building”, which is also another unit of measurement. The use of this unit can be

more suitable for the comparison with another measurable size, that of "total number of individuals that enters in the IT building".

Another requirement for the good measurement methodologies is that they mean something to the persons that examine them. They could reveal issues of infrastructure or service under review improving or demonstrating the value of persons and processes for the organisation. Even if the close relation to the general context does not constitute a main requirement for a good measurement, it helps to maintain measurement results inside the framework of the organisation under discussion while making the results more useful. This should benefit the end recipients (which are usually the management executives of organisation) to comprehend the current security status and decide with rational way based on results of the measurements.

As an example it can be mentioned the use of measurement as "the mean number of attacks" for the entire organisation. This measurement can have the all above characteristics (consistence, numerical price etc.) but it does not help anyone to improve his work. If this measurement is differentiated and connected with the enterprising services that it offers, as the servers of an electronic trade service, it will be a much more important tool for the decision-making process of more specific sectors, such as the protection of specific servers but also the physical protection of personnel.

3.5 Partial weight

The quantification of an individual factor that influences security is without a doubt very useful. Nevertheless, another important issue is the effect of these individual factors to the security of an entire organisation.

This characteristic is related with the previous paragraph ("Contextually Specific") due of the relativity that is implied between measurable sizes and the overall security of the organisation. It differs however in the fact that the requirement of overall estimation includes the way and the size with which a specific measurement influences the security and the operation of organisation.

As an example, the measurement of "numbers of power failures" is precise and relative to security. However, the way with which this measurement influences the operation of organisation can become also the weight of this particular size. Thus, in the case where there is no way to tackle a power failure (eg. A power generator) the weight of this measurement concerning the total estimate of security should be a large figure.

It should also be clarified that the requirement of an overall estimate could also be considered an extension of measurements, which could even require some form of calculation.

3.6 Repetitiveness

The requirement of repetitiveness includes the measurement of same factors while applying the same measurement methods in different time periods. This repetition aims in the verification of previous measurements as well as in the observation and recording of the evolution of a particular size.

Thus, this repetition should not constitute measurement from one only person but be also verified from the measurements of different persons.

Regarding the evolution of factors that are measured, the measurements should be performed periodically, in order to detect unexpected changes, or immediately after a particular known change which will probably influence security.

So, the measurements should be calculated with a frequency proportional with the rate of change of process. The methodologies that use samples at regular time intervals can help the organisations to analyze the effectiveness of security in precise time intervals and prepare them to be in the position to react in time in case of a new security incident. As expected, in a decision for whether a measurement should be calculated often, the cost of measurement should be taken into account in terms of time and money. Alternatively measurements could be performed only before and after each change.

3.7 Comparability

Also, it is very important that one should measure and observe the improvement or the deterioration of security as time advances. For this reason, the results of measurements should comparable to corresponding results of other organisations or different situations for the same organisation so that they can be contrasted to the current security status.

As reported above, a way to do that is to use common sizes and units of measurement. Additionally, is possible to measure in equivalent or relevant time periods points that share common characteristics, such as measurement of number of robberies during the last and first day of each month.

4. Taxonomy of existing security methodologies

Currently, there are several approaches for Security measurement. Most of them tend to emphasize on different aspects of security than objective measurements. There are very few approaches that focus on providing the means for quantifying security. The most noticeable solutions are:

- Solutions based on Vulnerability analysis
- Solutions based on Penetration testing
- Solutions based on Baseline comparison
- Solutions based on Best-practice and standards
- Solutions based on Risk management

4.1 Solutions based on vulnerability analysis

Solutions based on Vulnerability Analysis such as Microsoft Security Analyzer are connecting the security status of a networked system to the number its network-related vulnerabilities. Unfortunately vulnerability analyzers can not be used to measure security of

an entire organization because they do not take into account many factors such as operational flaws and personnel security. Moreover, the results are not related at all to the number of actual security incidents.

4.2 Solutions based on penetration testing

Solutions based on penetration testing such as Corsaire Testing, are following the exact same patterns of the attackers without causing real damage to the systems. However the presented outcomes of these approaches are more like subjective ratings and gratings than objective measurements. Additionally, they always focus on the technology related aspects of the organization and neglect other important factors such as operational and physical security.

4.3 Solutions based on baseline comparison

The baseline comparison solutions contain standard security controls, which are applicable to the great majority of IT systems providing basic security. The basis for the decision of whether the organization or specific service fulfils the security requirements is based on the Auditor's personal judgment.

The main issues regarding this kind of approach are that it is very subjective and tends to change every time the Auditor changes. Again the outcome is more like a rating than a proper measurement.

4.4. Solutions based on best-practice and standards

These solutions (e.g. ISO/IEC 17799, BS 7799 and NIST SP 800-33) refer to several suggestions for security countermeasures and controls to improve an organization's information security. Although these are approaches are quite thorough and explanatory, they are more useful when developing new infrastructures and services. So far the aspects of quantification and measurement have not been dealt with the same zeal.

4.5 Solutions based on risk management

These solutions assess security by describing, analyzing and evaluating single scenarios. Again, since the estimation of the risk is based on the Auditor's personal judgment, such solutions tend to be very subjective.

4.6 Combining the security's basic elements

Apart from the above categories two more categories of security measurement methodologies can be proposed. The first is concerned with the combination of security's basic elements. These basic elements are Integrity, Availability and Confidentiality. Other additional elements of IT Security are Non-Repudiation as well as Authentication.

An effort that could be included in this category is that of (Knorr, 2000). Within its framework, is proposed a structured approach for the analysis of metrics of security and for the quantification of the overall security of Electronic Business Applications. It uses a table that represents "overall security" and divides it to smaller parts. These parts correspond to

sites, potential targets and mechanisms of application security and are connected with the participating parts of an Electronic Business Application (customer, tradesman, means of communication). This process aims to the calculation of a quantifier of an Electronic Business Application, which functions as a means for the analysis, planning and comparison tool of similar applications.

Another approach that falls under this category is the one by (Serrelis, 2007) that aims to offer the foundation for a model that could help security analysts to quantify and measure security. Comparing to the requirements that were initially set, the suggested model has supported the consistency requirement throughout the document by the use of questions with objective answers. The questions also aimed to answers which would be cheap to gather, since the answers could come from automated systems such as IPSs. Additionally the model has managed to express security as a number (percentage). Security calculation has used at least one unit of measure (such as blocked spam emails) satisfying another requirement of a proper quantification model. The last requirement has also been covered since the level of security of the overall enterprise or the individual services makes a lot of sense to management people. Thus the model can also claim to be contextually specific. On the downside, it should be pointed out that the model is not considered so much with the new products, but with the existing services. Other type of questions should be posed to calculate the security level of new services and/or products.

4.7 Combining factors that are related to security

The second category of security measurement methodologies is concerned with the combination of factors that are related indirectly to security. Approaches of this type, even if of limited number, can be grouped together if they measure or calculate elements which are not directly related to security unlike the previous category. They aim to describe the relation between security and factors that are easily and objectively measured.

A typical example of this category is the approach that is presented in (Campbell, 2003), where the economic impact of incidents of security it is examined. The economic impact is translated in fall of the stock prices of an organisation, as a result of the negative image that is created in the investment public. Thus the stock price constitutes a factor which can indirectly be related to the level of security of organisation.

This approach has been an important factor for the development of the approach proposed and presented in paragraph 6, which also aims in the development of methodology for the objective measurement of security using factors that are related indirectly to security.

5. From measurement to calculation

As it is defined by Webster dictionary, calculation is “deliberate process for transforming one or more inputs into one or more results, with variable change”. The term calculation is used in numerous sciences, from the precisely defined arithmetic calculation to the calculation of abstract concepts which is implemented with the use of special algorithms and suitable combination of factors.

Another, alternative way of calculation of sizes is also the statistical analysis, eg. the calculation of likely results of an electoral result.

In every case the calculation of a factor is advisable in cases where his direct measurement or the quantification of its size is not feasible. These cases mainly include abstract concepts that are not straightly measurable, with security being a very representative example.

The calculation of security is differentiated from the measurement of security. While the measurement is based on the collection and representation of primary data, the calculation uses primary data with a combinational way so that it produces a result which represents security.

Because of the abstract nature of IT security, a direct measurement will not have real and usable results since it will be based on the limitations of the methods reported in the previou chapter. The calculation of however of security can be more efficient by overcoming these limitations using measurable sizes.

There are various methods for the calculation of security. These can depend on the judgments and estimates of researchers thus they are labelled as classifications or gradations. A second category of methods can be based on statistical methods, which could lead to an estimate of the level of security. Other methods can combine the measurement of values with the co-calculation of which the value of security could be deduced.

The optimum method of calculation of security is differentiated depending on the specific needs of each organisation, service, infrastructure or system. However, in all cases, it should be selected with a process that will be based on well defined factors that should also have well defined relations between them.

It should be also clarified that the methods of calculation and the methods of measurement of security do not constitute alternative solutions from each other, but complementary. Precise measurement of security should not be considered feasible, due to its abstract nature, but due to the fact that calculation of security cannot be reliable if it is not based on measurable factors. The researcher of security should therefore use measurement methodologies that would result measurable factors. From the combination of these sizes the value of security will also be deduced.

It becomes easily understood that the calculation of security can be realised with two ways. These are the quantification of non measurable factors and abstract significances, such as security and the use of measurable factors that are measured with the appropriate security measurement methodologies. The latter involve measurable factors and are applied as a type of quantitative analysis. Also, the level of security can result as an estimate of the researchers which is applied as a type of qualitative analysis.

6. A new quantification methodology

Within the framework of the current research, a new approach of calculation of security was also created, which manages security quantification methodology as a value which is calculated with the combination of certain easily measurable factors. These factors are

related indirectly with security as well as with the level of security of specific business services.

This approach is based on the principle that the abstract concepts can be calculated with the combination of factors that is related indirectly with them and themselves can be easily measured. At the same time it seeks the satisfaction of following general requirements:

- Appreciation of security as factor that is an important part of the business production environment and not a collateral issue with minimal or no operational interest.
- Usage and combination of factors that can be measured or be quantified with objective ways.
- Connection of results of calculation of security with the business decisions.

For the application of the particular methodology of calculation of security, the sources of primary data should be determined in order to be combined for security calculation. This particular methodology considers that the value of security can result from the combination of parameters that are related with it. The factors that were selected are five and they all concern certain business, functional or commercial value. These five factors are mentioned as CARLS from initial their names in the English language. These are:

- Compliance: It expresses the percentage of conformity with the legal and regulatory framework that is applicable to the business service.
- Availability: It expresses the percentage of uptime of service in comparison its mission time.
- Return: It expresses the size of profits that results from the particular service.
- Liabilities: It expresses the size of economic losses due to the particular service.
- Stock price: It expresses the price of stock of the company that offers the service.

All factors are essentially different aspects of business services and should be available in order be composed in a value that would represent the level of security for each of the business services. The usage of these specific factors has two basic advantages, which are the main reasons for their choice in this model.

The first advantage is the fact that all factors are already have been measured by organisations for reasons of operational evaluation. This means that there is no need for additional effort in order to assemble the information required. The second advantage is the fact that each factor provides an objective image of the organisation and its particular business services, which objectivity can not disputed.

The measurement and monitoring of all factors is considered essential for the development, viability and proper operation of each organisation. It is exceptionally usual, in the great majority of organisations, to monitor and collect all the above factors. In many cases these factors are also measured for each business service separately. This fact makes the collection

of the necessary elements a simple, easy and feasible process. Moreover, the CARLS factors have a lot more meaning for the persons that are found in not technical positions and their mentality is directed form the operational needs of their organisations. Compared to other approaches this can be seen as an advantage because using this methodology the understanding but also the usability of the value of security is facilitated which is based on familiar notions and no on technical terms as "integrity" and "confidentiality".

The main objective remains the calculation of the value of security of a specific service. This is implemented with the determination, the quantification and the combination of factors that can be measured easily and that is related indirectly with the security. This value portrays the level of security of specific service. The following paragraphs present the arguments in favour the choice of the particular factors, sating why CARLS factors are considered suitable for the calculation of security as well as an analysis for each one from them.

Compliance: The impact of non-compliance is profound. While many small issuers can operate with inconsistent compliance processes, problems eventually arise. Instead of focusing on the regulatory and punitive aspects of incomplete or ineffective compliance, this white paper will examine the functional impact of not remaining compliant with security regulations. Compliance can impact liquidity, which can affect your ability to raise funds for growth. The difficult aspect of compliance is knowing everything you have to do, when and how. Ongoing compliance requires an investment – for the same reasons as the initial compliance work you did when going public. The liquidity opportunities that initially attracted your company to the publicly traded arena are the same reasons for remaining compliant.

Availability: Government organizations and businesses of all sizes need to create and implement comprehensive business and operations continuity plans. Most organizations understand that they need to protect their data and systems -an activity known as disaster recovery. The disaster recovery is only half the battle-enterprises need also be prepared to quickly and seamlessly restart business processes in order to continue operations.

Return: The owners of a company and the company's creditors share a similar goal: to increase wealth. They are thus very concerned about profitability in all phases of operations. Creditors are specifically concerned that the company use its resources profitably so that it can pay interest and principal on its debt. Owners are concerned that the company be profitable so that stock values will increase. Company managers must show they can manage the owners' investment and produce the profits that owners and creditors demand. Because top management must meet the profit expectations of company owners, it passes down to the lower levels of management those profitability goals, which are then spread throughout the company. All managers, therefore, are expected to meet profitability goals, which are often increased and tightened as each level of management seeks a margin of security.

Liabilities: Most health related businesses would agree that securing insurance is one of the basic costs of doing business. As responsible business owners, they have budgeted for the appropriate coverages as a precautionary measure in the event of a loss— especially a catastrophic loss. However, there are a few optimistic souls who think of business insurance

as an option. These risk takers appear perfectly content to operate their salons with little or no coverage in place. Unfortunately, most financial experts agree that this is a very dangerous practice, as those who gamble and lose usually pay a much higher price in the long run. The bottom line is, while none of us ever expects to get sued, we've all got to accept that even the most adept operator may face litigation for any number of reasons. While there are a wide variety of insurance coverages available for protecting yourself and your business, one of the most essential is liability. Liability is an especially important issue for those in the tanning industry, whose business is providing customers a service which may pose some risk of injury to them. Liability risks come in many more forms than might be expected. In addition to liability arising specifically from the use of tanning equipment, salon owners also may be held accountable for a variety of other kinds of business liabilities, such as a customer slipping and falling.

Stock Market: By using a stock market return framework to examine the economic implications of information security breaches, [3] study contributes to the literature examining the economic effects of information security breaches. We find there evidence of an overall negative stock market reaction to announcements of information security. The economic cost of publicly announced information security breaches 445 breaches in major newspapers, although this finding is not robust across all specifications. Nevertheless, these results provide some support for the argument that information security breaches adversely affect the future economic performance of affected firms.

The choice of the above factors satisfies the two of the three basic requirements that had been placed within framework of the current approach of for the calculation of security, that is to say to appreciate security as a factor that is part of the business production environment as well as to use and combine measurable factors that can be quantified with objectively.

Based on the ideas described in the previous paragraph, a figure that would represent the level of security for a specific service should take into account all security factors presented. In order to mathematically express a formula that calculates security, several assumptions have been made.

Firstly, the notion of Target level for each factor is introduced. The target level is set by the upper management who is responsible for the overall operating constrains, such as security, of each business service offered. Within this context, the target level of Compliance, Availability, Returns and Stock Price are set. The target level of compliance can be the compliance to a specific industry directive or governmental law or even an international standard. Similarly, the target level of Availability should be defined taking into account the business needs of each service.

The Current level of Compliance will be represented as a "Yes" or "No" factor in order to keep the model as simple as possible. A future extension to that model can express the current compliance level as a percentage, signifying that a service does or does not cover all compliance needs (e.g. covers a law but not a specific international standard).

So, the Security figure for each service can expressed as a function of independent variables by the use of following formula:

$$S_S = \frac{C}{C_T} \times \frac{A}{A_T} \times \frac{R-L}{R_T} \times \frac{S}{S_T} \quad (1)$$

Where:

S_s = Security level of a Specific Business Service
C = Current Level of Compliance [0|1]
C_T = Target Level of Compliance (0-1]
A = Current Level of Availability [0…1]
A_T = Target Level of Availability [0…1]
R = Current Return of the Service (in a monetary value)
L = Current Liabilities of the Service (in a monetary value)
R_T = Target Return of the Service (in a monetary value)
S = Current Stock Price (Represents the company brand) (in a monetary value)
S_T = Target Stock Price (in a monetary value)

Having expressed security using the formula above, a proper usage of the results could be to a financial motivated one. Our target is to balance the spending in Security for each Business Service in order to maximize the organisation's Return on Investment:

$$\max ROI(S_1, S_2, ..., S_n) \quad (2)$$

subject to

$$\sum_{i=1}^{n} (R_i - I_i - L_i) > 0 \quad (3)$$

Where:

S_n = Security level of a Business Service
R_i = Revenues of a Business Service
I_i = Total Investments in a Business Service (Part of which is Security spending-investments)
L_i = Total Liabilities of a Business Service

Using the last formula another objective is achieved. This is the connection of results of calculation of security with the business decisions that are related to security investments. In other words this formula aims to answer the question whether a security investment would cost more than the expected benefits.

7. Conclusion

The question that was analyzed in this chapter is whether and how the principles of the security measurement methodologies can be applied so that the objective measurement of security of business services can be achieved. The motives that support this question are focused in the justification of expenses and investments that are related with to security. Thus, although the management of security is closely related to technical and organisational

level it is often difficult to define a quantified "version" of security that would be more comprehensible and usable in operational level.

This chapter also presents a critical evaluation and categorisation of the requirements of measurement and calculation methods of security, on which the restrictions of approaches that exist are based. Additionally a new security calculation approach is developed that attempts the quantification of security with the use of factors that are related indirectly to security.

The basic principle that was followed is that the research focus should be moved from the measurement of security to the calculation of security. Other principles were:

- Appreciation of security as factor that is an important part of the business production environment and not a collateral issue with minimal or no operational interest.
- Usage and combination of factors that can be measured or be quantified with objective ways.
- Connection of results of calculation of security with the business decisions.

The approach for the quantification of security is implemented via calculation. The variables that are used for the calculation are the CARLS factors, that is to say Compliance C with the legal and regulatory framework, Availability A of business services, Return R of each business service, Liabilities L due to specific services and the Stock price S of the organisation that reflects its fame and public image. The methodology supports that the security is mirrored in each one from these factors and hence the factors are related indirectly to that. This connection is expressed with a mathematic formula through the use of which the factors are considered equivalent.

An important advantage of the methodology is that through its use the management executives can comprehend more immediately the values that are produced by this and evaluate better where they should focus and support the security investments. This is particularly important because Security is an abstract concept which it is not easy to eb expressed as a measurable value.

One of the restrictions of method is the fact that the all factors they are considered equivalent during the calculation of security. A future research could investigate further the degree that security is influenced from every parameter as well as how this is altered in terms of service, organisation or market type.

8. References

Danahy, J. (2004) The Need for Metrics and Measurement in Application Security, OWASP Metrics and Measurement Standards

Fisher, D. (2009) Experts call for better measurement of security, Blog, recovered: 14/6/09, http://www.threatpost.com/blogs/experts-call-better-measurement-security

Sonnenreich, W.; Albanese, J. & Stout, B. (2006) Return On Security Investment (ROSI) – A Practical Quantitative Model, Journal of Research and Practice in Information Technology, Vol. 38, No. 1, February 2006

Maizlitsh, B. & Handler, R. (2005) IT Portfolio Management: Step by Step, John Wiley & Sons, ISBN: 978-0-471-64984-7, US

Sommerville, I. (1996) Software Engineering, Fifth Edition, Addison-Westley, ISBN: 978-0201427653, UK

Tipton, H. & Krause, M. (2008) Information Security Management Handbook, Sixth edition, Auerbach Publications, ISBN 978-1420067088

Olzak, T. (2007) The Pros and Cons of Security Risk Management, Tech Republic, recovered: 14/6/09, http://blogs.techrepublic.com.com/security/?p=180

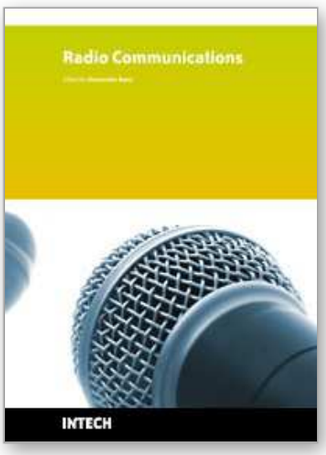
Parker, D. (2007) Risks of risk-based security, Communications of the ACM, Volume 50, Issue 3 , March 2007, pp 120.

Jaquith, A. (2007) Security Metrics: Replacing Fear, Uncertainty, and Doubt, Addison-Wesley Professional, ISBN 978-0321349989

Campbell, K.; Gordon, L. A.; Loeb, M. P. & Zhou L. (2003) The economic cost of publicly announced information security breaches: empirical evidence from the stock market, Journal of Computer Security, Volume 11, Issue 3 (March 2003) pp 431–448

Serrelis, Em. & Alexandris, N (2007) An Empirical Model for Quantifying Security Based on Services, IEEE Computer Society, Proceedings of the International Multi-Conference on Computing in the Global Information Technology, pp 30

Knorr, K.; Rohrig, S. (2000) Security of Electronic Business Applications: Structure and Quantification, Proceedings of the 1st International Conference on Electronic Commerce and Web Technologies EC-Web 2000, pp 25-37



Radio Communications

Edited by Alessandro Bazzi

ISBN 978-953-307-091-9
Hard cover, 712 pages
Publisher InTech
Published online 01, April, 2010
Published in print edition April, 2010

In the last decades the restless evolution of information and communication technologies (ICT) brought to a deep transformation of our habits. The growth of the Internet and the advances in hardware and software implementations modified our way to communicate and to share information. In this book, an overview of the major issues faced today by researchers in the field of radio communications is given through 35 high quality chapters written by specialists working in universities and research centers all over the world. Various aspects will be deeply discussed: channel modeling, beamforming, multiple antennas, cooperative networks, opportunistic scheduling, advanced admission control, handover management, systems performance assessment, routing issues in mobility conditions, localization, web security. Advanced techniques for the radio resource management will be discussed both in single and multiple radio technologies; either in infrastructure, mesh or ad hoc networks.

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

IntechOpen